L8: Entry 1 of 2 File: USPT Mar 2, 2004

DOCUMENT-IDENTIFIER: US 6698653 B1
TITLE: Identification method, especially for airport security and the like

Brief Summary Text (2):
Our present invention relates to an identification method, especially for airport security and the like which can be used for passenger identification, baggage/passenger matching, neonate identification, weapons identification, visa and passport applications, events security at sports events, conventions, amusement parks and theme parks, access control in a variety of facilities and for driver licenses, vehicle registration and the like and even for rapid ticketing, especially for airports and the like.

Brief Summary Text (13):
Another object of the invention is to provide an improved airport security system which will provide assurance that only baggage associated with an actual passenger is placed aboard an aircraft which can provide positive identification of a passenger to prevent substitution or fraud or criminal or terrorist activity, to ensure positive baggage identification upon termination of a flight and to ensure security within the airport at all stages from entry into the facility through check-in, boarding and baggage retrieval.

Brief Summary Text (19):
The invention has also been found to be particularly advantageous since it allows not only security at an airport or other facility in which limited accessibility is important, but because it can also significantly increase productivity at such facilities and wherever identification of a passenger and dispensing or sale of a ticket is required.

Brief Summary Text (21):
Passengers are able to immediately secure their boarding passes and baggage tags from the dispenser along with the ticket, without having to wait on check-in lines. The passenger can then affix the tag to the baggage and place the baggage on a nearby conveyor system for automated routing to the aircraft. The passenger can then proceed directly to the departure gate. If the passenger's luggage is placed at a secure location prior to dispensing of the boarding pass, the baggage tag bearing the microchip of the invention can be readily applied directly to the baggage. Indeed, wherever there is a suspicion that baggage tags may be inappropriately used, a chip bearing the biometric passenger identification may be provided directly to the baggage, unseen by the passenger, in addition to the baggage tag. Any mismatch of the chip on the baggage tag and the chip on the baggage can be readily ascertained on scanning.

Brief Summary Text (31):
An air traveler is enrolled in the security system at initial check-in (i.e. counter or curbside) when the passenger presents a ticket and identifies himself or herself as a passenger. The check-in enrollment point, equipped with a network workstation, uses live video frame capture and advanced facial recognition software to track, locate and extract the passenger facial image to a cropped digital photo. In cases where multiple faces are within the camera's visual field, the touch screen flat panel monitor will be utilized by the check-in personnel to manually

locate the eyes of the desired enrollee and automated enrollment will then follow. A duplicate copy of the digital photo as well as passenger profiling and the flight schedule generated at the workstation is sent to the network server database for storage and translation. Positive identification of the passenger's face is based upon the unique facial geometry from the stored photo image. Advanced facial recognition algorithms convert the unique facial geometry from the stored photo image into a biometric code or "face print". The algorithms containing the biometric code drawing on the uniqueness of the individual it was taken from are, by nature of their complexity, a natural encryption.

Brief Summary Text (32):
The encrypted biometric object becomes a sortable field in the server database where indexed sorts make quick work of rapid search and matching during successive passenger lookups. Passenger enrollment continues at the check workstation where the digital photo is converted to a compressed digital image file using the latest in image compression technology. The compressed image data file is destructively written (OTP) to the smart card (passive RF transponder) chip memory along with passenger information and the flight schedule. The encoded smart card carrying unique passenger information is permanently affixed to the passenger's boarding pass as well as identical smart card tags attached to each baggage item checked. The passenger enrollment process is finalized when a digital photo is sent to one or more databases controlled by the FBI, INTERPOL, or other law enforcement organizations. Once law enforcement organizations acquire the photo file from the server, they can use facial recognition software to rapidly compare for a positive match with photos of known terrorists. If there is a positive match, airport security can detain the suspect before he enters the security area or boards the aircraft.

Brief Summary Text (33):
After check-in, the baggage is sorted with RF smart card readers via the existing conveyor system that has been retrofitted with smart card readers to scan the luggage tags before loading onto the aircraft. The digital photos stored on the baggage tags are transmitted to the network server. The passenger proceeds to the carry-on security station where his digital facial image is again captured and compared with the images of passengers stored on the network server database in order to confirm that the individual entering the secure area is a registered passenger. The passenger then proceeds onward to the boarding gate. The passenger data now stored on the network server is accessible by the computer terminal at the boarding gate. The seamless noninvasive process is completed when the passenger will arrive at the gate with the boarding pass, whereupon the affixed smart card coming into proximity of the excitors/readers will be scanned (memory contents read). The compressed photo images previously extracted and stored from the baggage tag smart card memory and the real-time photo image extracted from the boarding pass smart card memory are decompressed and displayed on the network gate workstation. The photo image data read are passed back to the server for the internal rendering or biometric code of the stored facial image and compared. A split-screen Graphical User Interface (GUI) displays the facial images captured. The system software will automatically notify security personnel if the two images being validated at the boarding gate via the facial recognition software do not agree. To further enhance the security environment, a video image of the passenger can be captured at the boarding gate and compared with the existing images already stored on the server, boarding pass and baggage tags. This final comparison serves as a fail-safe means of assuring that the individual boarding the plane is the same person who originally presented and identified himself or herself at the check-in counter. In the event that the passenger will change planes at another airport, the same gate access and positive passenger baggage matching procedures will be employed.

Brief Summary Text (34):
Upon arrival at the final airport destination, the passenger baggage can be

recovered using a match of the passenger images stored in the baggage tag and boarding pass smart cards as the identifiers.

Detailed Description Text (2):
As can be seen from FIG. 1, the microchip 10 can be affixed to a foil strip 11 provided with a loop 12 serving as an antenna (antenna printed to smart card label laminate material) and enabling the microchip 10, which is a single use E-PROM to be inscribed with data from a remote terminal or by mounting the microchip, on a suitable carrier, in a holder of the terminal or otherwise. FIG. 1 shows the strip 11 greatly enlarged in scale and customarily the strip will be mounted on an identification object such as a boarding pass, baggage tag, bracelet, identity card, driver's license or the like which can be referred to as a "Smart Card", and on which the microchip will be hardly noticeable or even visible.

Detailed Description Text (4):
In the baggage match system of the invention (see FIG. 2), the facial image of the passenger is captured and data representing a biometric analysis of the triangle centered on the eyes and nose portion of the face is used to permanently encode smart card tags with the image and passenger information. The baggage tag and boarding pass for matching chips and the passenger's image is stored and compared with law enforcement security data bases. This is represented at 20 in FIG. 2.

Detailed Description Text (7):
FIG. 5 shows the basic system of the invention for baggage check-in and processing. As is customary for airport check-in, a number of check-in stations 50, 51 can be provided with respective baggage scales 52, flat panel screens 53 connected to the computer system, keyboard and mouse terminals 54, a smart card reader 55 and a device 56 for exciting the smart card and recording data thereon. A memory or image pick-up is represented at 57 at each station.

Detailed Description Text (8):
FIG. 5, at a lower portion shows the network layout with a baggage-sorting monitor station 60, the monitor 61 connected to the usual server 62, the data base system 63 and the various other equipment connected to the database. This can include a scanner/reader antenna 64 which is optional and such antennas can be provided at any location at the airport to effect general scanning of smart cards carried by individuals.

Detailed Description Text (10):
The processing of the passenger has been represented in the diagram of FIG. 6. When the passenger arrives at the airport 70, he or she can present himself or herself to a check-in point 71 which can be at curbside or a ticket counter (see FIG. 5). The passenger is queried for information and can be required to show a photo I.D., passport or the like which may previously have been encoded in the form of a smart card so that the recorded image can be matched to a face which is stored in a national or other database. He may be asked if he has packed his own luggage and whether that luggage has remained under his control the entire time since packing.

Detailed Description Text (12):
If baggage tags have been obtained at curbside, the facial data stored is automatically verified by the software comparing the recorded image and the image of the passenger presenting himself to the check-in facility. If there is an image by the visual recognition software at 72 of all of the items required to be in consonance, the facial recognition is stored at 73 in the server and the stored data is associated at 74 with flight schedules, passenger profiles and the like. The security check at 75 utilizing a law-enforcement database then follows and a security decision is made at 76 should the security check turn up a suspect. If the passenger is cleared, smart cards are permanently encoded at 77 with the compressed image of the passenger, data as to the passenger and flight schedule and baggage tags are applied at 78 to all items of baggage including carry-on luggage.

Naturally, if baggage tags have previously been affixed, they need not be duplicated here. The baggage is subjected to sorting and inspecting at 79.

Detailed Description Text (13):
The passenger proceeds to Security Checkpoint 1 where a live video capture of passenger is compared with data base of registered passengers to ensure that only passengers are permitted within the security zone. Thereafter, the passenger proceeds to final boarding at the gate 81, where the boarding ensues. In the final boarding at the gate 80, where the boarding pass is scanned and the image and data stored on the boarding pass is compared to the images encoded on the baggage tags and transmitted to the server and optionally with an image picked up by the CDD camera at the boarding station. Flight verification is effected at 82 and if the passenger is on the wrong flight, he or she is rerouted at 83 and the gate check is repeated at the new gate. If the passenger is on the correct flight, the baggage data is checked against the boarding passenger data at 84 and boarding is permitted at 85.

Detailed Description Text (14):
The airport security system of the invention has a number of advantages. For example, the use of contactless (RF) smart card technology with approximately IK bits writable memory allows the storage of a compressed facial image. RF communication is effected with the chip by the reader/scanner, eliminating the need for "line-of-sight" reads, as required by bar code technology. Therefore, the placement or positioning of the passenger baggage on conveyor systems or enrollment points is not a critical issue. Moreover, the RF communication protocol, particularly when used with higher frequencies such as 2.45 GHz, permits our system to read through nonmetallic baggage, thereby further enhancing the ability of CyberID to operate under less than optimal "real world" conditions. The passenger enrollment process is non-invasive and automated, unlike other identification systems that do not employ biometric facial recognition. The noisy electrical environment at airports will have no effect on the system and contactless communication with the RF microchips can be effected as distances greater than 12 inches from the reader, permitting scanning of baggage in a hold of an aircraft or in other locations with a portable reader. Chip data security is ensured because of the one-time programmable (OTP) nature of the chip.

Detailed Description Text (23):
Bag tags 132 (see also FIG. 3) are issued with compressed facial image storage in the embedded microchip and at 133 the boarding pass is issued (see FIG. 4) with its compressed facial image. Data as to ticketing information, passenger demographics and the like are then seen, with the compressed images to the main frame computer for the security checks at 134 and a ticket printer scanner system at 135 can generate the boarding passes and baggage tags and can provide the boarding pass itself as an E-ticket. The passenger can apply the baggage tags at 136 to the baggage in response to an instruction given at 137 to that effect. The passenger is warned to have the boarding pass available for scanning or presentation at the security checkpoint and boarding gate as represented at 138 and can then enter the security procedure at 139 (see FIGS. 5 and 6). When the passenger is released at the arriving airport, the boarding pass and the baggage tags can be disposed of by the passenger.

Previous Doc Next Doc Go to Doc#

L8: Entry 2 of 2 File: USPT Nov 17, 1998

DOCUMENT-IDENTIFIER: US 5838812 A
TITLE: Tokenless biometric transaction authorization system

Assignee Name (1):
SmartTouch, LLC

Assignee Group (1):
SmartTouch, LLC Berkeley CA 02

Brief Summary Text (5):
As verification of user identity is based solely on data placed on the token, which can be easily reproduced and transferred between individuals, such security must rely on both the diligence and the luck of the authorized user and merchant in maintaining this information as proprietary. However, by their very nature, tokens do not have a very strong connection with the individual. Identification of the rightful owner of the token through the token is tenuous at best. This is easily demonstrated by the fact that individuals other than the rightful owners of the tokens have been using these tokens to defraud merchants and other consumer goods suppliers.

Brief Summary Text (12):
In the near future, the banking industry expects to move to an even more expensive card, called a "smart card". Smart cards contain as much computing power as did some of the first home computers. Current cost projections for a first-generation smart card is estimated at approximately $3.50, not including distribution costs, which is significantly higher than the $0.30 plastic card blank.

Brief Summary Text (13):
This significant increase in cost has forced the industry to look for new ways of using the power in the smart card in addition to simple transaction authorization. It is envisioned that in addition to storing credit and debit account numbers, smart cards may also store phone numbers, frequent flyer miles, coupons obtained from stores, a transaction history, electronic cash usable at tollbooths and on public transit systems, as well as the customer's name, vital statistics, and perhaps even medical records. Clearly, the financial industry trend is to further establish use of tokens.

Brief Summary Text (14):
The side effect of increasing the capabilities of the smart card is centralization of functions. The flip side of increased functionality is increased vulnerability. Given the number of functions that the smart card will be performing, the loss or damage of this monster card will be excruciatingly inconvenient for the cardholder. Being without such a card will financially incapacitate the cardholder until it is replaced. Additionally, losing a card full of electronic cash will also result in a real financial loss as well. Furthermore, ability of counterfeiters to one day copy a smartcard is not addressed.

Brief Summary Text (15):

Unfortunately, because of the projected concentration of functions onto the smart card, the cardholder is left more vulnerable to the loss or destruction of the card itself. Thus, after spending vast sums of money, the resulting system will be more secure, but threatens to levy heavier and heavier penalties for destruction or loss of this card on the consumer.

Brief Summary Text (16):
The financial industry recognizes the security issues associated with smartcards, and efforts are currently underway to make each plastic card difficult to counterfeit. Billions of dollars will be spent in the next five years in attempts to make plastic ever more secure. To date, the consumer financial transaction industry has had a simple equation to balance: in order to reduce fraud, the cost of the card must increase.

Brief Summary Text (41):
In this manner, commercial transactions are conducted without the buyer having to use any portable man-made memory devices such as smartcards or magnetic stripe cards.

Brief Summary Text (63):
Yet another object of the invention is to provide a system of secured access that is practical, convenient, and easy to use, since individuals no longer need to write down their PINs in order to remember them.

Brief Summary Text (64):
Still another object of the invention is to provide a system of secured access to a computer system that is highly resistant to fraudulent access attempts by non-authorized users.

Detailed Description Text (2):
As noted, the main objective of this invention is to provide a tokenless, secure, reliable, safe, and consistent, apparatus and method, for identifying individuals for the purpose of performing financial transactions and non-financial transmissions, which can accommodate large numbers of users. It is the essence of this invention that consumers have the ability to conduct these transactions without the use of any tokens, credit cards, badges or identification cards including drivers licenses. In order to be functional it is important that the system operate at speeds required for completing financial transactions such as credit card purchases and ATM services, from multiple banks and credit accounts. The system must be secure, such that individuals records and their biometrics information remain confidential and safe, both within the computer system that identifies the individual and authorizes transactions, or during transfer of data between the computer system and remote sites with which the computer system communicates. Furthermore, the system must be reliable in that errors in identification and authorization must not hamper or make use of the system cumbersome. Since only the use of biometrics are contemplated for identification of individuals, the system must also have security measures to either reduce access, even to the authorized user, or notify authorities in emergency cases. It is appreciated that the system must be able to handle a large number of users, and accommodate storage and transfer of large amounts of data, such as bio-characteristic information, commensurate with speeds at which financial transactions are carried on today.

Detailed Description Text (443):
Note that only the biometric-related transactions are described in detail here. It is assumed that the RPT will also consist of standard credit and debit magnetic stripe card readers, as well as optional smart card readers too.

Detailed Description Text (454):
optional smart card reader (known in the industry)

L9: Entry 1 of 1 File: USPT Nov 17, 1998

DOCUMENT-IDENTIFIER: US 5838812 A
TITLE: Tokenless biometric transaction authorization system

Brief Summary Text (17):
In addition to and associated with the pervasiveness of electronic financial transactions, there is now the widespread use of electronic facsimiles, electronic mail messages and similar electronic communications. Similar to the problem of lack of proper identification of individuals for financial transactions is the problem of lack of proper identification of individuals for electronic transmissions. The ease and speed of electronic communication, and its low cost compared to conventional mail, has made it a method of choice for communication between individuals and businesses alike. This type of communication has expanded greatly and is expected to continue to expand. However, millions of electronic messages such as facsimiles and electronic mail (or "E-mail" or "email") messages are sent without knowing whether they arrive at their true destination or whether a certain individual actually sent or received that electronic message. Furthermore, there is no way to verify the identify the individual who sent or who received an electronic message.

Detailed Description Text (2):
As noted, the main objective of this invention is to provide a tokenless, secure, reliable, safe, and consistent, apparatus and method, for identifying individuals for the purpose of performing financial transactions and non-financial transmissions, which can accommodate large numbers of users. It is the essence of this invention that consumers have the ability to conduct these transactions without the use of any tokens, credit cards, badges or identification cards including drivers licenses. In order to be functional it is important that the system operate at speeds required for completing financial transactions such as credit card purchases and ATM services, from multiple banks and credit accounts. The system must be secure, such that individuals records and their biometrics information remain confidential and safe, both within the computer system that identifies the individual and authorizes transactions, or during transfer of data between the computer system and remote sites with which the computer system communicates. Furthermore, the system must be reliable in that errors in identification and authorization must not hamper or make use of the system cumbersome. Since only the use of biometrics are contemplated for identification of individuals, the system must also have security measures to either reduce access, even to the authorized user, or notify authorities in emergency cases. It is appreciated that the system must be able to handle a large number of users, and accommodate storage and transfer of large amounts of data, such as bio-characteristic information, commensurate with speeds at which financial transactions are carried on today.

Detailed Description Text (69):
High-speed DSP processor containing both flash and mask ROM

Detailed Description Text (634):
Each CST is connected to the system via a high speed local area network connection

such as token ring, ethernet, fiber (FDDI), etc. Each CST has the capability to query each of the databases, and display the results of these queries. However, the CST only displays fields and records based on the privilege of the individual terminal user. For instance, a standard customer service employee won't be able to see the encryption code for a given BIA's VDB record, though they can see which merchant or individual currently owns that BIA.

Previous Doc Next Doc Go to Doc#

L4: Entry 1 of 1 File: USPT Aug 15, 2000

DOCUMENT-IDENTIFIER: US 6105010 A
TITLE: Biometric certifying authorities

Brief Summary Text (9):
Recently, access to electronic services has been facilitated through identification and security techniques using biometric certificates, such as described in U.S. patent application No. 60/046,012, entitled "BIOMETRIC CERTIFICATES" by Clyde Musgrave et al., which is incorporated herein by reference. Such biometric certificates are useful to authenticate the identity of a person and to bind the biometric of the person to a transaction via a digital certificate. Such biometric certificates may be used as a spoof-proof method for recognizing individuals within an end-to-end secure electronic transaction.

Detailed Description Text (11):
Upon receiving the verification message 26 and/or the security level code, the certifying authority processor 28 generates a response to the transaction requester 12. If the verification message 26 indicates authentication of or a failure to authenticate the biometric certificate 18, the certifying authority processor 28 generates an access or denial message 32, respectively. In one embodiment, the access or denial message 32 is sent to the transaction requester 12 for further processing of the transaction request 14. The access or denial message 32 may merely be a logic 1 or TRUE Boolean value indicating access granted, or a logic 0 or FALSE Boolean value indicating a denial of access. Alternatively, the access or denial message 32 may include a report on confidence of the authenticity, such as a percentage value indicating the percentage of confidence in the authenticity for an access indication, or lack thereof for a denial indication.

Detailed Description Text (22):
The next lower level of the hierarchy 38 includes physical security BCAs 64 such as automobile access BCAs 66 and door access BCAs 68 for providing biometric certificates for car doors, building and office doors, residences, etc. Such BCAs may be disposed at the physical location, such as being built into the body of an automobile, or may be remote such as being implemented by a central security station of an office building or laboratory. In addition, such physical security BCAs 64 may be implemented in airports and individual airplanes for use in or supplemental to the verification of alleged passengers prior to boarding an airplane. On a scale of 1 to 10, the physical security BCAs 64 may be assigned a security value of 2.

Detailed Description Text (24):
In addition, individual entities may request and/or pay the BCA manager 10 to set higher and/or lower security values. For example, instead of a security value of 8.8, an institution such as "CHASE MANHATTAN BANK" may pay a fee to have a security value of 9.5, to not only have greater security in electronic fund transfers but also to be able to advertise that their transactions are more secure than transactions of competitor banks. Alternatively, regulatory agencies may mandate that certain entities, such as banks, have a requisite minimum security level for BCAs within the hierarchy 38. Further, such regulatory agencies may require certain

entities advertise and otherwise inform consumers of the security ratings of transactions. For example, the Federal Trade Commission (FTC) may mandate that automobile makers, such as "FORD MOTOR COMPANY", inform automobile purchasers or renters that their "FORD" automobiles either lack a BCA system for physical security and access, or have a predetermined BCA security rating.

Detailed Description Text (43):
The current needs of the marketplace involve check cashing facilities which take a portion of the face value or a fixed fee of each check cashed. The type of checks are typically government entitlement programs such Medicare, Medicaid, Social Security, Aid to Dependent Children, Food Stamps, Veteran's benefits, etc. The size of fraud in the Medicare and Medicaid programs alone is estimated at over $40 Billion. A portion of this fraud is attributable to check cashing fraud and lack of positive identification of the persons involved.

CLAIMS:

1. A biometric certifying authority (BCA) management system comprising:

a transaction request parser for receiving a request to authenticate an electronic transaction having transaction-type data and a biometric certificate signal, the request parser operating to extract the biometric certificate signal and the transaction-type data from the request;

a biometric verification processor which receives the biometric certificate signal, determines an authenticity of the biometric certificate signal based on previously stored biometric data in a database, and based on the determination, generates a verification comprising one of an authentic status and a fraudulent status of the biometric certificate signal;

a transaction type classifier for receiving the transaction type data and for determining a security level associated with the electronic transaction based on at least one of the transaction-type data and a predetermined hierarchy of electronic transactions; and

a certifying authority processor for generating an access-or-denial message based on at least one of the verification and the security level.

Previous Doc Next Doc Go to Doc#

L6: Entry 1 of 1 File: USPT Aug 15, 2000

DOCUMENT-IDENTIFIER: US 6105010 A
TITLE: Biometric certifying authorities

Detailed Description Text (52):
Biometric certificates fit well in this scenario, since biometric certificates create a new standard for secure identification (ID) methods. Electronic commerce in this scenario is keyed to cashless smartcards, with guaranteed security and insured validation of every transaction. Since cyberspace is relatively new, standards/laws for the cyberspace marketplace and commerce are evolving, and so cyberspace is ideal for experimenting with new paradigms.

L2: Entry 1 of 1 File: USPT Aug 15, 2000

DOCUMENT-IDENTIFIER: US 6105010 A
TITLE: Biometric certifying authorities

Brief Summary Text (3):
This disclosure relates generally to the field of secure communications, and in particular to the issuance and management of biometric certificates in a hierarchy of biometric security systems.

Brief Summary Text (5):
Electronic transactions may involve diverse types of activities, such as the exchange of information, the permitted entry and access of a person to a facility, and the output of goods or cash to a person. Despite the common need for security, different activities may have different levels of security, and so different activities may utilized different security techniques.

Brief Summary Text (6):
Existing certifying techniques, such as personal certificates employing, for example, passwords and personal information numbers (PINs), have not provided sufficient security since PINs and passwords are often easily guessed, hard to remember, and/or subject to exhaustive or brute-force automated searches.

Brief Summary Text (9):
Recently, access to electronic services has been facilitated through identification and security techniques using biometric certificates, such as described in U.S. patent application No. 60/046,012, entitled "BIOMETRIC CERTIFICATES" by Clyde Musgrave et al., which is incorporated herein by reference. Such biometric certificates are useful to authenticate the identity of a person and to bind the biometric of the person to a transaction via a digital certificate. Such biometric certificates may be used as a spoof-proof method for recognizing individuals within an end-to-end secure electronic transaction.

Brief Summary Text (10):
As different electronic transactions may require different levels of security, a need exists for controlling the generating, distributing, revoking, and maintaining of biometric certificates through one or more biometric certifying authorities (BCAs). Such a BCA control system should provide insurability of issued biometric certificates for different electronic transactions.

Brief Summary Text (12):
It is recognized herein that a hierarchical approach and evaluation procedure for the issuance of biometric certificates insures specific levels of security for specific types of electronic transactions.

Detailed Description Text (2):
Referring in specific detail to the drawings, with common reference numbers identifying similar or identical elements, steps, and features, as shown in FIG. 1, the present disclosure describes a biometric certifying authority management system and method of use for providing and maintaining a hierarchical relationship among

biometric certifying authorities in the issuance of biometric certificates. The hierarchical approach and evaluation procedure in the issuance of biometric certificates insures specific levels of security for specific types of electronic transactions.

Detailed Description Text (10):
The transaction type data 20 is sent from the request parser 16 to a transaction type classifier 30 to determine the type of transaction and the corresponding level of security required of the transaction, according to a predetermined hierarchy shown, for example, in FIG. 2. The transaction request 14 may include a transaction code as the transaction type data 20 for indicating the type of transaction involved. The transaction type classifier 30 may then compare the transaction code with a set of predetermined transaction codes which may be stored, for example, in a transaction code table or database. The transaction type classifier 30 may then generate a security level code which is output to the certifying authority processor 28.

Detailed Description Text (11):
Upon receiving the verification message 26 and/or the security level code, the certifying authority processor 28 generates a response to the transaction requester 12. If the verification message 26 indicates authentication of or a failure to authenticate the biometric certificate 18, the certifying authority processor 28 generates an access or denial message 32, respectively. In one embodiment, the access or denial message 32 is sent to the transaction requester 12 for further processing of the transaction request 14. The access or denial message 32 may merely be a logic 1 or TRUE Boolean value indicating access granted, or a logic 0 or FALSE Boolean value indicating a denial of access. Alternatively, the access or denial message 32 may include a report on confidence of the authenticity, such as a percentage value indicating the percentage of confidence in the authenticity for an access indication, or lack thereof for a denial indication.

Detailed Description Text (13):
In conjunction with or independent of the access or denial message 32, the certifying authority processor may access a billing rate database 34 for generating a bill 36 or charge for the process of verifying and/or for providing a report on the confidence of the authentication or lack thereof. The billing rate database 34 may also include a table or database of insurance rates for charging the transaction requester 12, in the bill 36, to indicate a level of insurance commensurate with a level of security insured by a positive authentication by the BCA manager 10. Alternatively, the billing rate database 34 may specify a percentage of the transaction amount or value involved.

Detailed Description Text (15):
The bill 36 with the insurance charge may be in the form of a credit card transaction pre-authorized by the transaction requester 12 as a pre-established authentication and insurance service with the BCA manager 10. In this manner, the BCA manager 10 exchanges guarantees of authentication for payment of insurance and/or authentication charges, and so electronic transactions may be conducted with greater assurance of security and authenticity.

Detailed Description Text (16):
As shown in FIG. 2, the transaction type classifier 30 may classify transactions from different BCAs according to the predetermined hierarchy 38 of electronic transactions and BCAs conducting such electronic transactions. For example, all BCAs shown in FIG. 2 may be associated with a root BCA 40 having the highest degree of security. The root BCA 40 may have associated therewith electronic transactions involving governmental and national security BCAs 42 as well as various digital and biometric certifying authority administrative BCAs 44. Such BCAs merit the greatest levels of security and correspondingly the greatest security values, since such BCAs 42, 44 involve agencies and systems which monitor and secure other electronic

systems such as other BCAs.

Detailed Description Text (17):
For example, on a scale of 1 to 10, the BCAs 42, 44 in the root BCA 40 may be assigned a security value of 10, requiring the greatest accuracy in authentication of biometric certificates in electronic transactions.

Detailed Description Text (18):
The next lower level of the hierarchy 38 includes electronic fund transfer BCAs 46 such as banking BCAs 48 and securities BCAs 50 for providing biometric certificates involved in secure electronic transactions of money, money-related entities, and money-related information. On a scale of 1 to 10, the electronic fund transfer BCAs 46 may be assigned a security value of 8.

Detailed Description Text (19):
The next lower level of the hierarchy 38 includes insurance transaction BCAs 52 such as bonding BCAs 54 and surety BCAs 56 for providing biometric certificates for secure electronic transactions involving, for example, insurance and guarantee payment contracts. On a scale of 1 to 10, the insurance transaction BCAs 52 may be assigned a security value of 6.

Detailed Description Text (21):
lading, electronic letters of credit, etc. On a scale of 1 to 10, the business purchase BCAs 58 may be assigned a security value of 4.

Detailed Description Text (22):
The next lower level of the hierarchy 38 includes physical security BCAs 64 such as automobile access BCAs 66 and door access BCAs 68 for providing biometric certificates for car doors, building and office doors, residences, etc. Such BCAs may be disposed at the physical location, such as being built into the body of an automobile, or may be remote such as being implemented by a central security station of an office building or laboratory. In addition, such physical security BCAs 64 may be implemented in airports and individual airplanes for use in or supplemental to the verification of alleged passengers prior to boarding an airplane. On a scale of 1 to 10, the physical security BCAs 64 may be assigned a security value of 2.

Detailed Description Text (23):
It is understood that the list of BCAs in the hierarchy 38 is not exhaustive and that the order of the BCAs may be implemented in different configurations, provided that each type of BCA is associated with a security value. In addition, individual BCAs within a specific type of BCA may be differentiated with unique or diverse security values. For example, within the electronic fund transfer BCAs 46, the banking BCAs may be assigned security values of 8.8 while the securities BCAs may be assigned security values of 8.4, such that banking transactions are required to be more secure than securities transactions, and so are charged more for authentication.

Detailed Description Text (24):
In addition, individual entities may request and/or pay the BCA manager 10 to set higher and/or lower security values. For example, instead of a security value of 8.8, an institution such as "CHASE MANHATTAN BANK" may pay a fee to have a security value of 9.5, to not only have greater security in electronic fund transfers but also to be able to advertise that their transactions are more secure than transactions of competitor banks. Alternatively, regulatory agencies may mandate that certain entities, such as banks, have a requisite minimum security level for BCAs within the hierarchy 38. Further, such regulatory agencies may require certain entities advertise and otherwise inform consumers of the security ratings of transactions. For example, the Federal Trade Commission (FTC) may mandate that automobile makers, such as "FORD MOTOR COMPANY", inform automobile purchasers or

renters that their "FORD" automobiles either lack a BCA system for physical security and access, or have a predetermined BCA security rating.

Detailed Description Text (25):
For businesses in general, there are about $10 million to about $100 million in fraud reserve funds collected and maintained annually. Business generally have about 100,000 to 500,000 electronic transactions per month, with fraud levels amounting from about $10 million to about $100 million annually. Generally, about 10,000 to 100,000 participants are involved in electronic transactions, with a market size greater than $1 billion per year. Accordingly, to implement BCA managers 10 and the BCA security hierarchy 38, businesses are clearly able to support the costs of biometric certificate hardware and software.

Detailed Description Text (42):
The security concerns of such electronic transactions is problematic, since there is generally a lack of uniform identification in large segments of the population. About $1 billion to $2 billion in check cashing transaction fees per year are collected, with fraud levels at about 10%.

Detailed Description Text (43):
The current needs of the marketplace involve check cashing facilities which take a portion of the face value or a fixed fee of each check cashed. The type of checks are typically government entitlement programs such Medicare, Medicaid, Social Security, Aid to Dependent Children, Food Stamps, Veteran's benefits, etc. The size of fraud in the Medicare and Medicaid programs alone is estimated at over $40 Billion. A portion of this fraud is attributable to check cashing fraud and lack of positive identification of the persons involved.

Detailed Description Text (52):
Biometric certificates fit well in this scenario, since biometric certificates create a new standard for secure identification (ID) methods. Electronic commerce in this scenario is keyed to cashless smartcards, with guaranteed security and insured validation of every transaction. Since cyberspace is relatively new, standards/laws for the cyberspace marketplace and commerce are evolving, and so cyberspace is ideal for experimenting with new paradigms.

Detailed Description Text (53):
The applications of biometric certificates using BCA managers 10 may be expanded to the government and the population, delivering biometric certificate security benefits after prototyping with the un-banked. Higher-value transactions may then be built and implemented, with nominal fees being charged such as $1.00 to $2.00 per transaction.

Detailed Description Text (70):
The needs of the marketplace for biometric certificates for subscription services include allowing customers to order products on credit electronically through a private network. The size of fraud in such subscription services is virtually unknown, but the approximate fraud exposure is about $10 million to $100 million. The lack of security prevents these companies from putting new and more valuable products up on their private networks. By putting new products up in a system with mutual trust using biometric certificates and the BCA manager 10, these companies are able to increase their per-transaction revenue and build a larger

CLAIMS:

1. A biometric certifying authority (BCA) management system comprising:

a transaction request parser for receiving a request to authenticate an electronic transaction having transaction-type data and a biometric certificate signal, the request parser operating to extract the biometric certificate signal and the

transaction-type data from the request;

a biometric verification processor which receives the biometric certificate signal, determines an authenticity of the biometric certificate signal based on previously stored biometric data in a database, and based on the determination, generates a verification comprising one of an authentic status and a fraudulent status of the biometric certificate signal;

a transaction type classifier for receiving the transaction type data and for determining a security level associated with the electronic transaction based on at least one of the transaction-type data and a predetermined hierarchy of electronic transactions; and

a certifying authority processor for generating an access-or-denial message based on at least one of the verification and the security level.

3. The BCA management system of claim 1 wherein the predetermined hierarchy is a list of rankings of BCAs according to predetermined security and authentication levels.

5. The BCA management system of claim 4 wherein the billing rate database stores billing rates which increase for corresponding transaction classifications having greater associated security and authentication levels.

7. A biometric certifying authority (BCA) management system for authenticating an electronic transaction request, including a biometric certificate signal and transaction-type data, comprising:

a biometric verification processor which receives a biometric certificate signal, verifies the biometric signal based on biometric data in a database, and generates a verification comprising one of an authentic status and a fraudulent status of the biometric certificate signal;

a transaction type classifier which receives the request and generates a security level associated with the electronic transaction based on at least one of the transaction-type data and a predetermined hierarchy of electronic transactions;

a billing rate database which stores a plurality of billing rates corresponding to a plurality of security levels; and

a certifying authority processor for generating an access-or-denial message based on at least the verification, the certifying authority processor further operative to retrieve a corresponding billing rate from the billing rate database, and to generate a bill in accordance with the billing rate for the access-or-denial message.

10. The BCA management system of claim 9 wherein the billing rate database stores billing rates which increase for corresponding transaction classifications having greater associated security and authentication levels.

11. The BCA management system of claim 7 wherein the predetermined hierarchy is a list of rankings of BCAs according to predetermined security and authentication levels.

12. The BCA management system of claim 11 wherein the predetermined hierarchy includes rankings of BCAs from a group including at least one of: root BCAs, electronic fund transfer BCAs, insurance BCAs, business purchase BCAs, and physical security BCAs.

16. The method of claim 15 wherein the predetermined hierarchy is a list of

rankings of biometric certifying authorities (BCAs) according to predetermined security and authentication levels.

17. The method of claim 16 wherein the predetermined hierarchy includes rankings of BCAs from a group including at least one of: root BCAs, electronic fund transfer BCAs, insurance BCAs, business purchase BCAs, and physical security BCAs.

19. The method of claim 13 wherein the step of storing includes the step of storing billing rates in the billing rate database, with the billing rates increasing for corresponding transaction classifications having greater associated security and authentication levels.

Previous Doc Next Doc Go to Doc#